M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

John A. Yanchunis
(Pro Hac Vice)
Ryan D. Maxey
(Pro Hac Vice)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Attorneys for Plaintiff

THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

KAMAL BITMOUNI, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

PAYSAFE PAYMENT PROCESSING SOLUTIONS LLC, a Delaware limited liability company,

Defendant.

Case No.: 3:21-cv-00641-JCS

SECOND AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Kamal Bitmouni ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Second Amended Class Action Complaint against Paysafe Payment Processing Solutions LLC ("Defendant"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' PII, including without limitation, names, contact details, Social Security numbers, and bank account information (collectively, "personal identifiable information" or "PII"). Plaintiff also alleges Defendant failed to provide timely, accurate, and adequate notice to Class Members that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. On or before November 6, 2020, Defendant obtained possession of some or all of Plaintiff's and Class Members' PII through unknown means and for purposes not yet known.

3. On or before November 6, 2020, Defendant shared some or all of the PII of Plaintiff and Class Members with one or more of its affiliates. Again, the reason or purpose for sharing this information is not yet known, although what is known is that information about consumers has become a valuable resource upon which businesses generate other business and/or profit.

4. In sharing some or all of the PII of Plaintiff and Class Members with one or more of its affiliates, Defendant had a duty to ensure that the shared PII was and would be properly secured.

5. On or before November 6, 2020, Defendant's affiliate, Paysafe Group Holdings Limited ("PGHL"), now known as PI UK HOLDCO 1 LIMITED, discovered a potential compromise of a website used by part of its U.S. business (the "Data Breach").

6. On or before December 3, 2020, PGHL determined that suspicious activity on the website from May 13, 2018 to November 24, 2020 may have compromised information held on the website.

7. On or around December 16, 2020, PGHL notified Plaintiff that his PII, including his name, contact details, Social Security number, and bank account information, may have been accessed during the Data Breach.[1]

8. On or around January 12, 2021, PGHL notified the Maine Attorney General that the PII of 91,706 individuals may have been accessed during the Data Breach.[2]

9. Maine law requires an information broker or any other person "who maintains computerized data that includes personal information" to notify Maine residents of "a breach of the security of the system." Me. Re. Stat. Ann. tit. 10, § 1348.1.

10. Maine law also requires that notice be provided to the Department of Professional and Financial Regulation or the Attorney General. *Id.* § 1348.5.

11. In notifying Maine residents and the Maine Attorney General of the Data Breach, PGHL indicated that it, alone or with others, maintained Plaintiff's and Class Members' PII at the time of the Data Breach.

12. In order for PGHL to have maintained Plaintiff's and Class Members' PII at the time of the Data Breach, it obtained some or all of the PII, directly or indirectly, from Defendant.

13. In order for any other affiliates of PGHL to have maintained Plaintiff's and Class Members' PII at the time of the Data Breach, such affiliates obtained the PII, directly or indirectly, from Defendant.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. Defendant, through its affiliate PGHL, admits that the unencrypted PII exposed to "unauthorized activity" included names, contact details, Social Security numbers, and bank account information.

15. The exposed PII of Plaintiff and Class Members can be sold on the dark web.

[1] Exhibit 1 (Redacted "Notice of Data Breach" provided to Plaintiff by Paysafe, dated December 16, 2020.)

[2] Exhibit 2 (Screenshot of the Maine Attorney General "Data Breach Notifications" website for Paysafe; *also available at*: https://apps.web.maine.gov/online/aeviewer/ME/40/19dd2b37-106a-4a4f-aa0e-76cf4008ec45.shtml (last accessed March 30, 2022).)

Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

16. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant, through its affiliate PGHL, waited over a month to report it to the states' Attorneys General and affected individuals.

17. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they are and continue to be at significant risk to identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

18. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes; and (iv) ensure that any affiliates of Defendant that directly or indirectly acquired some or all of the PII from Defendant did (i), (ii), and (iii).

19. Plaintiff and Class Members have suffered cognizable injuries as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII. Moreover,

Plaintiff and Class Members are at a present and increased risk of identity theft as a result of Defendant's conduct and failures as herein pled.

20. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. While a digital copy of the PII of Plaintiff and Class Members was taken, Plaintiff and Class Members have a continuing interest in ensuring that their information which remains in Defendant's possession is and remains safe, and they should be entitled to injunctive and other equitable relief to ensure that their information is protected.

II. PARTIES

21. Plaintiff Kamal Bitmouni is a Citizen of California residing in Chino Hills, California. Mr. Bitmouni received Defendant's *Notice of Data Breach*, dated December 16, 2020, on or about that date.

22. Defendant Paysafe Payment Processing Solutions LLC is a limited liability company organized under the laws of Delaware with a principal office in California at 30721 Russel Ranch Road, Suite 200, Westlake Village, California.

23. Defendant's sole member is Paysafe Holdings (US) Corp, a Delaware corporation.

24. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

25. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff (a citizen of California) and one or more of the 485 Maine residents who PGHL represented may have had their personal information impacted during the Data Breach,[3] is a citizen of a State different from Defendant, which is a citizen of Delaware.[4]

27. The Northern District of California has personal jurisdiction over Defendant named in this action because Defendant is organized under the laws of California and conducts substantial business in California and this District through itself and/or its subsidiaries.

28. Venue is proper in this District under 28 U.S.C. §1391(b) because California has more than one judicial district and Defendant's contacts in this District would be sufficient to subject it to personal jurisdiction if this District were a separate State.

IV. FACTUAL ALLEGATIONS

Background

29. Defendant services thousands of businesses in accepting and processing credit and debit payments.

30. Prior to the Data Breach, Defendant acquired the PII of some or all of Plaintiff and Class Members through unknown means.

31. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties and ensure that any affiliates with which

[3] Exhibit 3 ("Security Incident Notification," dated December 16, 2020, provided to Maine Attorney General by Paysafe).

[4] As a limited liability company, Defendant is "a citizen of every state of which its owners/members are citizens." *Johnson v. Columbia Props. Anchorage, LP*, 437 F.3d 894, 899 (9th Cir. 2006). Defendant is a citizen of Delaware because its sole member is a Delaware corporation, Paysafe Holdings (US) Corp.

Defendant directly or indirectly shared the PII also adopted reasonable measured to protect it.

The Data Breach

32. Beginning on or about December 16, 2020, Defendant sent Plaintiff and Class Members a *Notice of Data Breach*.[5] Defendant informed the recipients of the notice that:

> We are writing to inform you of a cybersecurity incident that may have affected personal information related to you. You provided the information to Merchant Services* in the course of enrolling for a merchant account.
>
> **WHAT HAPPENED** On November 6, 2020, through Merchant Services'* internal cybersecurity program, we discovered a potential compromise of a website used by part of our U.S. business. We promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, we identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. We created a secure environment to test the queries, using available logs and other information to assess potential impact. By November 19, 2020, we determined that a subset of the queries identified might have involved data held on the website. We analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and we engaged external forensics experts to assist. By December 3, 2020, we determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, we have identified evidence of suspicious activity on the website between May 13, 2018, and November 24, 2020. We have notified law enforcement. Although we are not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing your personal information, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.
>
> **WHAT INFORMATION WAS INVOLVED** The information about you that may have been accessed includes your name, contact details, Social Security number, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Merchant Services'* core processing and operating systems. The website was part of a legacy system used internally and by a small group of former Chi Payment agents, a group acquired in an

[5] *See* Exhibits 1 and 3.

> acquisition of iPayment in 2018, and contains certain data of a limited subset of merchants and agents.[6]

33. On or about December 16, 2020, Defendant began notifying various state Attorneys General, including Maines's Attorney General, signed by "Merchant Services."[7]

34. Defendant admitted in the *Notice of Data Breach* and the letters to the Attorneys General that one or more unauthorized third persons submitted automated queries to Defendant's website and that some of these queries could have returned information to unauthorized actors, including the names, contact details, Social Security numbers, and bank account information of Plaintiff and Class Members.

35. In response to the Data Breach, Defendant claims that it "took steps to prevent further unauthorized access and have closed the website. We continue to invest in cybersecurity, including enhancing our website scanning practices and vulnerability detection program. Additionally, we have arranged for you to obtain credit monitoring and identity monitoring services at no cost to you for two years through Kroll, a leading provider of credit monitoring and identity monitoring services."[8]

36. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing Plaintiff's and Class Members' PII to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.

38. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

39. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant

---

[6] Ex. 3, p. 3.
[7] Ex. 3, p. 4.
[8] Ex. 3, p. 3.

assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure and for ensuring that any affiliates with which it shared the PII would also protect the PII from disclosure.

40. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

Securing PII and Preventing Breaches

41. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII and ensuring any affiliates with which it directly or indirectly shared the PII also properly secured it. Or Defendant could have destroyed the data, especially old data that Defendant had no legal duty to retain.

42. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

43. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[10]

45. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

[9] 17 C.F.R. § 248.201 (2013).
[10] *Id*.

Value of Personal Identifiable Information

46. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

47. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

48. What is more, it is no easy task to change or cancel a stolen Social Security number.

---

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed March 30, 2022).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed March 30, 2022).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed March 30, 2022).

[14] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 30, 2022).

An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

49. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

50. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth.

51. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

52. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

53. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to others criminals who will purchase the PII for that purpose. The

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed March 30, 2022).

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed March 30, 2022).

fraudulent activity resulting from the Data Breach may not come to light for years.

54. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

55. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and Class Members' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's or its affiliate's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

56. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

57. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's or its affiliate's network, amounting to potentially tens of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

58. To date, Defendant's affiliate, PGHL, has offered Plaintiff and Class Members only two years of identity theft protection services through a single credit monitoring and identity monitoring service, Kroll. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

59. The injuries to Plaintiff and Class Members were directly and proximately caused

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed March 30, 2022).

by Defendant's failure to implement, maintain, and ensure adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Kamal Bitmouni's Experience

60. Mr. Bitmouni received the Notice of Data Breach, dated December 16, 2020, on or about that date.

61. On or about December 5, 2020, Plaintiff attempted to log into his personal checking account and discovered that he was denied access. He then contacted his bank and discovered that unknown, unauthorized third-parties had used Mr. Bitmouni's PII, including but not limited to his name, bank account information, and Social Security number, to access his checking account in an attempt to divert Mr. Bitmouni's funds and had requested an access code for the account from a device Plaintiff did not have access to or own.

62. Upon regaining access to his account, Plaintiff discovered that these unknown, unauthorized third parties had been in the process of diverting his funds from this account when he discovered their actions.

63. As part of this attempt to divert his funds, these unknown, unauthorized third parties stopped payments on a number of Plaintiff's scheduled payments, including a rental payment of $1,600.

64. Plaintiff had to exhaust more than eight hours communicating with his bank, landlord, and others to discover what happened and to attempt to resolve the fraud.

65. The delays caused by these "stopped payments" resulted in Plaintiff's rent being approximately forty-five (45) days late, as it took that many days for the bank to resolve the fraudulent activity.

66. As a result of the Data Breach notice and the unauthorized access to his checking account, Mr. Bitmouni spent time dealing with the consequences of the Data Breach, which includes time spent communicating with his bank to stop the fraudulent transfers, verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance

options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

67. The credit monitoring service provided by Defendant to Mr. Bitmouni warned him on or about January 13, 2021, that his PII is potentially exposed on the dark web.

68. Additionally, Mr. Bitmouni is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

69. Mr. Bitmouni stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

70. Mr. Bitmouni suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Bitmouni entrusted to Defendant for its services to accept payment card payments, which was compromised in and as a result of the Data Breach.

71. Mr. Bitmouni suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

72. Mr. Bitmouni has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and bank account information, being placed in the hands of unauthorized third-parties and possibly criminals.

73. Mr. Bitmouni has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

74. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

75. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals who are residents of the United States and whose PII was or may have been accessed during the cybersecurity incident referenced in the Notice of Data Breach dated December 16, 2020 that Merchant Services (including CHI Payments, iPayment, and Paysafe) sent to Plaintiff (the "Nationwide Class").

76. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Kamal Bitmouni asserts claims on behalf of a separate statewide subclass, defined as follows:

> All individuals who are residents of California and whose PII was or may have been accessed during the cybersecurity incident referenced in the Notice of Data Breach dated December 16, 2020 that Merchant Services (including CHI Payments, iPayment, and Paysafe) sent to Plaintiff (the "California Class").

77. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

78. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

79. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant's affiliate PGHL has identified tens of thousands of individuals whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. PGHL advised Maine's Attorney General that the Data Breach affected 91,706 individuals.

80. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class

Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members and ensure its affiliates adequately safeguarded the PII;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach and ensure its affiliates did the same;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur and ensured its affiliates did the same;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, nominal, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

81. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

82. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

83. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

84. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

85. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

86. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

87. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

88. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

89. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

90. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and ensure its affiliates with which it directly or indirectly shared the PII did the same;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and ensure its affiliates with which it directly or indirectly shared the PII did the same;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security and ensure its affiliates with which it directly or indirectly shared the PII did the same;

d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach and failed to ensure its affiliates with which it directly or indirectly shared the PII did the same;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members and failing to ensure its affiliates with which it directly or indirectly shared the PII did the same; and,

g. Whether Class Members are entitled to actual, consequential, nominal, and/or statutory damages and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

91. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

92. Plaintiff acquired and stored the PII of Plaintiff and Class Members and shared the PII, directly or indirectly, with its affiliates.

93. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

94. Defendant knew or reasonably should have known that the failure of Defendant or its affiliates to exercise due care in the collecting, storing, and using of Plaintiff's and Class Members' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

95. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties, including ensuring its affiliates did the same. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and ensuring its affiliates with which it directly or indirectly shared the PII did the same.

96. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Plaintiff's and Class Members' PII it was no longer required to retain pursuant to regulations and ensure its affiliates with which it directly or indirectly shared the PII did the same.

97. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII and ensure its affiliates with which it directly or indirectly shared the PII did the same.

98. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

99. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's and its affiliates' inadequate security practices.

100. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the

inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the necessity for encrypting PII stored on Defendant's systems, and the need to ensure its affiliates with which it directly or indirectly shared the PII did the same.

101. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendant, and its failure to ensure its affiliates with which it directly or indirectly shared the PII did the same.

102. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's or its affiliates' possession.

103. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

104. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

105. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members and ensure its affiliates with which it directly or indirectly shared the PII did the same.

106. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

107. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII

was within Defendant's possession or control and failing to ensure its affiliates with which it directly or indirectly shared the PII did the same.

108. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach and failed to ensure its affiliated with which it directly or indirectly shared the PII did the same

109. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect Plaintiff's and Class Members' PII in the face of increased risk of theft and failed to ensure its affiliates with which it directly or indirectly shared the PII did the same.

110. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII and failing to ensure its affiliates with which it directly or indirectly shared the PII did the same.

111. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Plaintiff's and Class Members' PII it was no longer required to retain pursuant to regulations and failing to ensure its affiliates with which it directly or indirectly shared the PII did the same.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach and failed to ensure its affiliates with which it directly or indirectly shared the PII did the same.

113. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

114. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members, and ensure its affiliates with which it directly or indirectly shared the PII did the same, and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was lost and accessed

as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures and failure to ensure its affiliates with which it directly or indirectly shared the PII did the same.

115. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

116. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein, and failing to ensure its affiliated with which it directly or indirectly shared the PII did the same. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and directly or indirectly shared with its affiliates and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

117. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

118. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

119. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

120. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and

attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's and its affiliate's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (viii) present and continuing costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

121. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

122. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

123. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

125. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third

parties.

126. Defendant owed a duty to Plaintiff and the Nationwide Class to keep their PII confidential.

127. Defendant failed to protect and directly or indirectly through its affiliates released to unknown and unauthorized third parties the PII of Plaintiff and the Nationwide Class.

128. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Nationwide Class the Nationwide Class, by way of Defendant's failure to protect the PII and failure to ensure its affiliates with which it directly or indirectly shared the PII did the same.

129. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

130. The intrusion was into a place or thing, which was private and is entitled to be private.

131. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

132. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its or its affiliates' information security practices were inadequate and insufficient.

133. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

134. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

135. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

136. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Violation of California's Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiff and the Nationwide Class)

137. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

138. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

139. Defendant stored the PII of Plaintiff and Class Members in its computer systems and directly or indirectly shared the PII with its affiliates, which stored the PII in their computer systems.

140. Defendant knew or should have known it and its affiliates did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.

141. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was vulnerable to hackers because Defendant's and its affiliates' data security measures were inadequate and outdated, and Defendant and its affiliates were the only ones in possession of that material information, which Defendant had a duty to disclose.

A. Unlawful Business Practices

142. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its and its affiliates' computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

143. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, by failing to ensure its affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely` notify Plaintiff and Class Members of the Data Breach.

144. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

145. Defendant's acts and omissions as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

146. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff's and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

B. Unfair Business Practices

147. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendants' and its affiliates' data security cannot be said

to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and Class Members, directly causing the harms alleged below.

148. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

149. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and Class Members' PII remains in Defendant's and its affiliates' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016)

(failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

150. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiff and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

151. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT IV
Violation of California's Consumer Privacy Act
(Cal. Civ. Code § 1798.150)
(On behalf of Plaintiff and the California Class)

152. Plaintiff and California Class members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

153. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and California Class members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Class members and failure to ensure its affiliates with which it directly or indirectly shared the PII did the same.

154. As a direct and proximate result of Defendant's acts, Plaintiff's and California Class members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

155. As a direct and proximate result of Defendant's acts, Plaintiff and California Class members were injured and lost money or property, including but not limited the loss of Plaintiff's and California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

156. Defendant knew or should have known that its or its affiliates' computer systems and data security practices were inadequate to safeguard Plaintiff's and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Class members and failed to ensure its affiliates with which it directly or indirectly shared the PII did the same.

157. Defendant is a corporation organized for the profit or financial benefit of its shareholders. Defendant collected Plaintiff's and the California Class's PII and/or PHI as defined in Cal. Civ. Code § 1798.140.

158. Defendant has a gross annual revenue of over $25 million and buys, receives, and/or sells the personal information of 50,000 or more California residents, households, or devices.

159. Pursuant to Section 1798.150(b) of the CCPA, Plaintiff gave written notice to Defendant of its violations of section 1798.150(a) by certified mail dated October 7, 2021.

160. Defendant, however, failed to "actually cure" its violations within 30 days of the written notice, and failed, pursuant to § 1798.150(b) to "provide[] the consumer an express written statement that the violations have been cured and that no further violations shall occur."

161. Defendant failed to "actually cure" its violations by, among other things, not encrypting Plaintiff's and the California Class's PII and/or PHI and by not deleting data it no longer had a reasonable need to maintain in an Internet accessible environment.

162. As a result, Plaintiff and California Class members seek relief under § 1798.150(a), including, but not limited to, statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief

the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members'

personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees'

compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: March 30, 2022

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 300263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

JOHN A. YANCHUNIS
(*Pro Hac Vice*)
RYAN D. MAXEY
(*Pro Hac Vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Attorneys for Plaintiff